Appendix 305A

FEDWIRE DISCUSSION - Excerpts from the Federal Financial Institutions Examination Counsel's Information Systems Examiner's Guide

Fedwire is the Federal Reserve System's nation-wide electronic funds and securities transfer net-work. Fedwire links the 12 Federal Reserve Banks with the many depository institutions that maintain reserve or clearing accounts with the Federal Reserve. Fedwire processes approximately $1.4 trillion in funds and securities transfers each day. It provides for the electronic transfer of **immediate** and **irrevocable** payments between participating institutions, and functions as both a clearing and settlement facility. The Fedwire book-entry securities transfer system provides for the transfer of U.S. government and federal agency securities that settle on the books of the Federal Reserve.

Fedwire may be accessed by direct computer interface, or off-line by telephone through a PC-based electronic system called Fedline. Fedline was developed by the Reserve Banks and uses dial-up lines for network access.

The Fedwire funds transfer system is a credit transfer system. Each funds transfer is settled individually on the books of the Federal Reserve as it is processed, and is considered a **final and irrevocable** payment. When a corporate sends a funds transfer request, it **irrevocably** authorizes its Reserve Bank to debit (charge) its account for the settlement account, and further authorizes the Reserve Bank of the receiving institution to give credit in the same amount to the payee. The Federal Reserve guarantees immediate availability of funds; once the Federal Reserve bank credits the receiving institution's account or delivers the advice of payment, the Federal Reserve Bank will not reverse credit for the payment. Therefore, there is no settlement risk to the recipient of a Fedwire Transfer. The Federal Reserve Bank assumes the risk only if the sending institution overdraws its position at the Reserve Bank.

The Federal Reserve's payments system risk policies are designed to limit the risk that a financial institution fails with its reserve account overdrawn. Reserve Banks require that depository institutions continuously monitor and adjust their reserve account positions to ensure adequate funds are on hand, or that they are in compliance with established overdraft limits and collateral requirements.

Other risks associated with Fedwire funds transfers include potential loss due to errors, omissions, and fraud. Corporates are expected to have internal controls and segregation of duties sufficient to reasonably ensure that the risk of loss from these risks is minimized.

FEDLINE TERMINAL SECURITY MEASURES

1. THE LOCAL SECURITY ADMINISTRATOR

The Local Security Administrator (LSA) is responsible for setting up new users on the local Fedline system. The LSA also is responsible for setting the function levels of all users. The LSA is a powerful user and has the tools to bypass all security and effectively send a transfer with no supervision if other compensating controls, such as limited access to the terminal, prompt balancing, and timely activity log review are not in effect.

The LSA should be someone who has NO day-to-day operational duties on the Fedline terminal. The LSA's main purpose is to add new users and change function security levels. Anytime the LSA uses the terminal, a member of the operations staff should be present to monitor his/her actions. If the Fedline terminal has a power on password, it should be implemented and the password restricted from the LSA. In addition, the LSA should not have a host access logon (HC) at the Federal Reserve host mainframe computer. Not having host communications prevents the LSA from logging onto the host mainframe and sending a transfer. (However, the LSA could queue a funds transfer (TQ status), and the next time a valid transfer exchange was made, the unauthorized transfer would be sent automatically.)

The LSA with unrestricted access could perform the following functions to bypass security and send a funds transfer without involvement by a second individual:

a) add two new user ID's with enter and verify capability, and then effect a transfer single - handily.

b) change the verification rule to "N," thus eliminating the verification requirement.

c) change the verification threshold dollar amount to $99,999,999.99, thus circumventing the verification requirements.

2. THE MISCELLANEOUS SECURITY SETTINGS

The Fedline Miscellaneous Security Settings will be reviewed at every examination. The settings are as follows:

a) User ID suspended - Consecutive bad password retries

This setting specifies the maximum number of consecutive invalid sign-on attempts operators can make before the local user ID is suspended. This prevents an unauthorized person from trying to guess the password of a legitimate user by limiting the number of invalid password retries. ***The Federal Reserve Board's recommended setting is 3.***

b) Users must periodically change their password every XX days

This setting Specifies the maximum number of days operators can use their password before they must change it. ***The Federal Reserve Board's recommended setting is 30.***

c) Verification rule

This setting determines the message verification requirement, which requires that more than one person be involved with the processing of all transfers completed on the system. Three options are available, N, U, and E (see the description of the option settings below**). The Federal Reserve Board's recommended setting is E, however U is acceptable.**

1) *N - No restriction (Very high risk)* This option allows the operator who entered and/or updated a message also to verify that same message. There is no dual control of any funds transfer if this option is chosen. For example, Joe enters message. He also can update and verify that same message.

2) *U - Verifying operator cannot be the last operator who updated the transfer*. This option prevents the last operator who entered or updated a transfer from verifying that same message. It would allow the original operator to verify the transfer if it was changed by a second operator. For example, Joe enters a transfer and Paul updates (changes) that same message. Paul cannot verify that same message, but Joe can.

3) *E - The verifying operator cannot be operator who entered or updated the transfer*. This option prevents any operator who entered or updated a transfer from verifying that same transfer. For example, Mary enters a transfer and Paul updates that same transfer. Neither Mary nor Paul can verify that same message. A third operator with has verification authority must verify the transfer.

d) Override and release rule

This field is used to indicate the level of restrictions placed on overriding and/or releasing transfers. This potentially allows users to bypass verification. Only operators with *supervisor function* access level have the ability to perform the Override & Release function. Three options - N, U, or E - are also available for the override and release rule. ***The Federal Reserve Board's recommended setting is E.***

1) *N - No restriction on override or release*. Any operator with the supervisor function access level can override or release the verification of a transfer regardless of any previous processing performed.

2) *U - Limited restriction on override or release.* The operator overriding or releasing the transfer cannot be the operator who last updated the message. (This setting may be considered by smaller corporates with limited staff.)

3) *E - Full restriction.* The operator releasing the transfer cannot be the operator who updated or who originally entered the message.

e) Time-out Intervals

This parameter minimizes the amount of time that a terminal remains active if a user forgets to sign-off. It causes the system to revert to the Fedline Sign-on screen after a specified amount of time passes in which no keystrokes have been entered. **The Federal Reserve Board's recommended setting is 10 minutes.**

f) Cycle-Date rollover and Print-delete option

Before the beginning of each day's work, a function must be performed on the Fedline terminal known as the "cycle date rollover." The purpose of this function is to reset the date on the terminal. The Fedline system requires the operator to clear or cancel any messages that are still pending (i.e. - have been initiated but not verified/ transmitted) before performing this function. If any messages are pending, requiring an operator to cancel them in order to complete the cycle date rollover, policies should require that a record of these messages be reported to management. The software is originally set on "Full" as the default.

1) *FULL* - Prints a full recap report of the previous days funds transfers before they are deleted by the cleanup cycle data mode change program.

2) *SUMMARY* - Prints an abbreviated report of the previous days funds transfers before they are deleted by the cleanup cycle date mode change program.

It is recommended that this option be set in the FULL account option so that a complete detailed record is on file and can be reviewed.

g) Suppression of the Check for Possible Keyboard Eavesdropping

This option on the system allows the administrator turn off or keep on the "Possible Keyboard Eavesdropping" message each time the system is entered. It is recommended that this option be kept on to assure that no other software on the system is affecting the Fedline II software.

3. THE USER/ACCESS REPORT

The user access report lists the various capabilities of each Fedline user. The report will be reviewed to determine that no one person can effect a funds transfer, and that access levels

on all Fedline applications are limited to what users must have to do their job. Corporates have a tendency toward having multiple "back-ups" in case of absence, etc. and having the back-up staff with active access on Fedline. Excessive "back-up" personnel with continuous Fedline access should be discouraged.

The following additional controls should be observed in review of user/access levels.

a) The Local Administrator (LA) function should not have access to the funds transfer (FT) application or host communications (HC). In fact, there is no reason for the LA to have any other available applications beyond LA. Note: There is no way to determine conclusively at the corporate if any user has host access. This can only be determined by calling the data security department of the respective Federal Reserve Bank. The presence of the host communications (HC) under their user ID is usually a good indicator, but not conclusive since the LSA could use the "Master ID" to activate the HC application at any time.

b) No user should have more than one user ID. Doing so would enable the individual to enter a funds transfer using the first ID, then log back on and verify and send the message using the second ID.

c) No more than two staff members should be assigned as Local Administrators. The Federal Reserve Guidelines suggest an Administrator and one backup administrator.

d) No funds transfer staff should have the Funds Transfer "Supervisor" or "Manager" function. These functions have access levels that can be used to bypass the verification requirement. These access levels should only be activated by the Local Administrator in unusual circumstances. The LA should monitor the actions performed using these access levels and then de-activate the access levels when the action is completed. Note: It is possible that the supervisor function may be needed in some Fedline applications such as Start-up/Shutdown. However, it is not normally needed in funds transfer.

4. THE VERIFICATION FIELDS

The "update funds application attributes" option allows staff members with "Manager" function level or the LA to set the verification fields and applicable verification thresholds for funds transfers. Verification means fields must be re-keyed by a second operator. If none of the fields has an "X" next to them, none have to be re-keyed. However, a second operator still has to call up the transfer on the screen and review it prior to releasing it.

Available options range from no verification of any field to required verification of every field. Between these two extremes, management and/or the LA can select individual fields that would be required to be verified. At a minimum, verification of the dollar amount should be required.

Verification thresholds allow the corporate to set a dollar amount over which all funds transfers must be verified. Normally, the threshold should be set at $0.00, which requires verification of all funds transfers. If the verification level is set at a higher amount, this amount should be approved by the board of directors and noted in the minutes. There should also be compelling reasons why management does not want to have all funds transfers require review by a second operator prior to being sent.

5. GENERAL CONTROLS

a) The "master" User-ID

It could occur that a local administration function needs to be performed but no LA is available. In case of such a situation, the "master" user-ID password should be stored in a secure location should the corporate need to access it. In no case should any operating personnel be able to access the "master" password individually. It should be under dual custody, preferably in a lock box with dual keys/combinations.

b) Configuration Diskette

This diskette is used by the corporate, in conjunction with the Federal Reserve, if for some reason everyone is locked out of the system. The configuration diskette should also be stored in a secure location under dual custody.

c) Power On Password

Most micro-computers have a power on password feature, which requires that a password be input before the computer will activate. If the Fedline terminal has this feature available, it should be activated. If a power on password is activated, it should not be disclosed to the local administrator. This would preclude the local administrator performing unauthorized system changes and/or transfers.